

WHAT IS CLAIMED IS:

- 1           1.       A method of providing security for a computer connected to a data store, the  
2 method comprising the steps of:  
3           receiving an authentication key, a user name, and a computer identifier;  
4           parsing the authentication key to obtain a parsed user name and computer identifier;  
5 and  
6           validating the received user name and computer identifier using the parsed user name  
7 and computer identifier.
- 1           2.       The method of claim 1, wherein validating comprises determining whether the  
2 received user name and computer identifier match the parsed user name and computer  
3 identifier.
- 1           3.       The method of claim 2, wherein a match indicates that the received user name  
2 and computer identifier are valid.
- 1           4.       The method of claim 1, further comprising, before parsing, decrypting the  
2 authentication key.
- 1           5.       The method of claim 1, further comprising, if the received user name and  
2 computer identifier are valid, logging onto a server connected to the computer with a server  
3 user identifier and server password.
- 1           6.       The method of claim 5, further comprising, parsing the authentication key to  
2 obtain the server user identifier and server password.
- 1           7.       The method of claim 6, wherein multiple users share one server user identifier  
2 and server password.

1           8.     The method of claim 1, further comprising generating the authentication key.

1           9.     The method of claim 8, wherein the computer is connected to a client and a  
2 server and wherein the authentication key is generated with a client user name, a client  
3 computer identifier, a server user identifier, and a server password.

1           10.    The method of claim 8, further comprising encrypting the authentication key.

1           11.    The method of claim 8, further comprising forwarding the authentication key  
2 to a user.

1           12.    The method of claim 1, wherein the computer is connected to a client and a  
2 server, and further comprising:

3               at the client, transmitting the authentication key, a client user name, and a client  
4 computer identifier to the server; and

5               at the computer,

6               intercepting the authentication key; and

7               if the user name and computer identifier are valid, logging onto the server.

1           13.    An apparatus for providing security, comprising:

2               a computer having a data store connected thereto;

1               one or more computer programs, performed by the computer, for receiving an

2 authentication key, a user name, and a computer identifier, parsing the authentication key to

3 obtain a parsed user name and computer identifier, and validating the received user name and

4 computer identifier using the parsed user name and computer identifier.

1           14.    The apparatus of claim 13, wherein validating comprises determining whether  
2 the received user name and computer identifier match the parsed user name and computer  
3 identifier.

1           15.     The apparatus of claim 14, wherein a match indicates that the received user  
2     name and computer identifier are valid.

1           16.     The apparatus of claim 13, further comprising, before parsing, decrypting the  
2     authentication key.

1           17.     The apparatus of claim 13, further comprising, if the received user name and  
2     computer identifier are valid, logging onto a server connected to the computer with a server  
3     user identifier and server password.

1           18.     The apparatus of claim 17, further comprising, parsing the authentication key  
2     to obtain the server user identifier and server password.

1           19.     The apparatus of claim 18, wherein multiple users share one server user  
2     identifier and server password.

1           20.     The apparatus of claim 13, further comprising generating the authentication  
2     key.

1           21.     The apparatus of claim 20, wherein the computer is connected to a client and a  
2     server and wherein the authentication key is generated with a client user name, a client  
3     computer identifier, a server user identifier, and a server password.

1           22.     The apparatus of claim 20, further comprising encrypting the authentication  
2     key.

1           23.     The apparatus of claim 20, further comprising forwarding the authentication  
2     key to a user.

1           24.    The apparatus of claim 13, wherein the computer is connected to a client and a  
2 server, and further comprising:

3                   at the client, transmitting the authentication key, a client user name, and a client  
4 computer identifier to the server; and

5                   at the computer,

6                   intercepting the authentication key; and

7                   if the user name and computer identifier are valid, logging onto the server.

1           25.    An article of manufacture comprising a computer program carrier readable by  
2 a computer and embodying one or more instructions executable by the computer to perform  
3 method steps for providing security to the computer connected to a data store, the method

4                   receiving an authentication key, a user name, and a computer identifier;

5                   parsing the authentication key to obtain a parsed user name and computer identifier;

6                   and

7                   validating the received user name and computer identifier using the parsed user name  
8 and computer identifier.

1           26.    The article of manufacture of claim 25, wherein validating comprises  
2 determining whether the received user name and computer identifier match the parsed user  
3 name and computer identifier.

1           27.    The article of manufacture of claim 26, wherein a match indicates that the  
2 received user name and computer identifier are valid.

1           28.    The article of manufacture of claim 25, further comprising, before parsing,  
2 decrypting the authentication key.

1           29.    The article of manufacture of claim 25, further comprising, if the received user  
2 name and computer identifier are valid, logging onto a server connected to the computer with  
3 a server user identifier and server password.



1           30.     The article of manufacture of claim 29, further comprising, parsing the  
2 authentication key to obtain the server user identifier and server password.

1           31.     The article of manufacture of claim 30, wherein multiple users share one  
2 server user identifier and server password.

1           32.     The article of manufacture of claim 25, further comprising generating the  
2 authentication key.

1           33.     The article of manufacture of claim 32, wherein the computer is connected to  
2 a client and a server and wherein the authentication key is generated with a client user name,  
3 a client computer identifier, a server user identifier, and a server password.

1           34.     The article of manufacture of claim 32, further comprising encrypting the  
2 authentication key.

1           35.     The article of manufacture of claim 32, further comprising forwarding the  
2 authentication key to a user.

1           36.     The article of manufacture of claim 25, wherein the computer is connected to  
2 a client and a server, and further comprising:

3                 at the client, transmitting the authentication key, a client user name, and a client  
4 computer identifier to the server; and

5                 at the computer,

6                         intercepting the authentication key; and

7                         if the user name and computer identifier are valid, logging onto the server.